4.6. DISEÑO DE SEGUIMIENTO Y AUDITORÍA

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

4.6.1. Auditoria del SIC. El siguiente diseño de auditoría proporciona una herramienta para la verificación del funcionamiento del SIC, y el satisfactorio cumplimento de todas sus funcionalidades tanto técnicas como procedimentales, también permite evaluar el correcto cumplimiento de las políticas, estándares y normatividad de la Registraduría Nacional del Estado Civil.

El diseño de la presente auditoría proporciona la base para evaluar el sistema de control interno de la organización, en lo que respecta al área de sistemas.

El diseño de la auditoría se basa en listas de chequeo y cuestionarios de control interno, que permiten obtener información concreta respecto al tema de interés.

Cuadro 342: Lista de chequeo comprobar los niveles de seguridad del sistema.

LISTA DE CHEQUEO	SI/NO/N.A. Ref P/T
Área: Dependencias donde este en funcionamiento el SIC. **Actividad:** Comprobar los niveles de seguridad del sistema.	
¿Se cuenta con un documento oficial que relacione los usuarios de los diferentes sistemas de la Entidad así como el respectivo nivel de atribución dentro de los mismos?	
¿Las claves de acceso (contraseñas) al sistema son únicas para cada usuario?	
¿Se inhabilitan oportunamente las claves de acceso del personal que se ausenta temporal o definitivamente de sus labores en la Empresa?	
¿Se inhabilitan oportunamente las claves de acceso del personal que se ausenta temporal o definitivamente de sus labores en la Empresa?	
¿Son confidenciales y restrictivas las claves de acceso de los usuarios?	
¿Permite el sistema individualizar las operaciones de adición, modificación, consulta, borrado y reporte de información dentro de las opciones del sistema y asignar estas operaciones a usuarios específicos?	
¿Permite el sistema restringir el acceso de procesos o acciones específicas del sistema a usuarios no autorizados?	
¿Se encuentran implementadas dentro del sistema de seguridad tales restricciones?	
¿Se encuentra implementado el cambio periódico y forzoso de las claves de acceso a todos los usuarios del sistema?	
¿Controla el sistema un número determinado de intentos de acceso al sistema?	
¿El administrador de seguridad del sistema lleva un control periódico de los usuarios que se ausentan temporal o definitivamente de la Entidad a fin de inhabilitarlos?	
¿Se cuenta con procedimientos claros para los casos en que los usuarios olviden su clave de acceso?	
¿Se inhabilitan dentro del sistema las claves de acceso asignadas a usuarios retirados de la Empresa?	
¿Cuenta el sistema con un archivo de pistas de auditoría que registre las acciones efectuadas por los	

usuarios dentro del sistema?	
¿Impide el sistema que el Administrador pueda conocer las claves de acceso de los demás usuarios?	
¿Existe sólo un único empleado con privilegios especiales de administración del sistema?	

Cuadro 343: Lista de chequeo revisar seguridad en los archivos electrónicos y bases de datos.

LISTA DE CHEQUEO	SI/NO/N.A. Ref P/T
Área: Dependencias donde este en funcionamiento el SIC. **Actividad:** Revisar seguridad en los archivos electrónicos y bases de datos.	
¿Existe un manual que describa el contenido y la estructura de los archivos de datos?	
¿Se cuenta con un manual que describa los procedimientos para el mantenimiento (depuración, fusión, corte, copia de respaldo) de los archivos de datos que posee el sistema?	
Dejan los procesos ejecutados evidencias de: ▪ Fecha de ejecución ▪ Nombre y/o número de trabajo ▪ Nombre y/o número del programa ▪ Hora de iniciación y terminación del mismo ▪ Archivos utilizados	
¿Permite el sistema a los operadores y/o usuarios en general, manipular los archivos tipo reporte?	
¿Es restringido el acceso a este tipo de archivos? Se llevan controles adicionales (supervisión de procesos, restricciones de acceso al sistema operativo, eliminación de comandos peligrosos dentro del sistema operativo) para impedir la adulteración de información arrojada por el sistema mediante reportes en medio magnético?	
¿Se cuenta con una única persona responsable de llevar a cabo las copias de respaldo?	
¿Se cuenta con una política de copias de respaldo dentro de la Empresa?	